IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

FIRST SENIOR FINANCIAL GROUP, LLC et al.	:	
	:	
Plaintiffs,	:	CIVIL ACTION
	:	
v.	:	NO. 12-cv-1247
	:	
"WATCHDOG" et al.	:	
	:	
Defendants.	:	

DEFENDANT WATCHDOG'S BRIEF IN OPPOSITION TO PLAINTIFFS' MOTION FOR SANCTIONS BASED ON "SPOLIATION OF EVIDENCE"

Defendant Watchdog hereby files this brief in opposition to Plaintiffs' Motion for Sanctions Based on "Spoliation of Evidence" (Doc. No. 134).

I. INTRODUCTION

On July 7, 2013, when Plaintiffs allege that Watchdog wiped her mother's computer, Watchdog was verifiably more than 1,300 miles away from it.[1] As such, Plaintiffs cannot meet the most fundamental requirements in the spoliation analysis—control over the evidence, actual suppression of it, and bad faith. But even if Plaintiffs could prove these elements, they would still fail to show that there was evidence on the computer in the first place; that any evidence was relevant; and that there was a reasonably foreseeable duty to preserve. In the remote circumstance that Plaintiffs prove liability, they would also fail to show prejudice or that any of their proposed sanctions are appropriate. Plaintiffs' motion, which seeks judgment against

[1] That Watchdog could not have accessed the Target Computer on July 7, 2013 should not come as a surprise to Plaintiffs—as Watchdog advised them that she was forced to move out of her mother's house prior to that date on several occasions. (See Doc. No. 111 at 5, 7, 8; Doc. No. 111-1 at 5, 6, 7, 31; Doc. No. 112 at 5, 7, 8; Doc. No. 112-1 at 5, 6, 7, 31.)

Watchdog, is actually just a crude attempt to dam the flood of evidence washing their defamation case away. (See generally Doc. No. 82-1; Doc. No. 116; Doc. No. 117; Doc. No. 132-2.)

II. FACTS

Watchdog created the truthaboutcannella.com web site on January 17, 2011. (Doc. No. 82-3 at 2.) She created the truthaboutcannella.net web site on March 10, 2011. (Id.) These web sites contained truthful information about Plaintiffs' unethical and illegal business practices in the insurance market for retirees. (See generally Doc. No. 82-1; Doc. No. 116; Doc. No. 117; Doc. No. 132-2.)

Plaintiffs filed a Complaint in this Court on March 9, 2012. (See Doc. No. 1.) Plaintiffs alleged that Watchdog violated the Lanham Act and intentionally interfered with their existing and prospective business relations. (See id.) They also sought an injunction to take down Watchdog's web site. (See id. at 15-16.)

On July 31, 2012, 145 days after Plaintiffs filed their original Complaint, they filed a Verified First Amended Complaint ("FAC") (Doc. No. 9) against Watchdog and nine other anonymous defendants. (See id.) Plaintiffs did not seek the consent of the Court or any of their ten opponents before filing the FAC. In the FAC, Plaintiffs allege Lanham Act violations, defamation, tortious interference with business relationships, and civil conspiracy. (See id.)

No later than August 1, 2012, Plaintiffs were working with Bruce Anderson, a cyber investigator and Certified Digital Forensics Engineer. (See Doc. No. 10-3; Doc. No. 87-1; Doc. No. 90-1.) Mr. Anderson is knowledgeable about computer forensic examinations. (See Doc. No. 90-1.)

On August 30, 2012, the Court authorized Plaintiffs to effect service of the FAC and summons on Watchdog by e-mailing those documents to two addresses. (See Doc. No. 17.) Plaintiffs did not serve Watchdog at these addresses. (See Doc. No. 48; Doc. No. 83 at 10; Doc. No. 83-2 at 1, 4; Doc. No. 116 at 7.) The summons allegedly emailed to Watchdog lacked the Court's seal. (See Doc. No. 82-2 at 3.) Watchdog never received Plaintiffs' alleged service e-mail. (See Doc. No. 82-3 at 3.) See also Fifth Decl. of Krista C. Brennan ¶ 3, Nov. 7, 2013, attached hereto as Exhibit A.

On October 4, 2012, Plaintiffs requested that the Clerk enter a default against Watchdog. (See Doc. No. 49.) The Clerk entered default on the same day. (See Docket.) Four days later, Plaintiffs moved for a default judgment against Watchdog. (See Doc. No. 50.) On November 16, 2012, the Court entered default judgment against Watchdog. (See Doc. No. 56.)

Watchdog did not learn of this action or of the default judgment until mid-December 2012, at which point she began searching for counsel. See Ex. A at ¶ 3. (See also Doc. No. 82-3 at 4.) On February 15, 2013, Watchdog filed a motion to vacate the default and default judgment. (See Doc. No. 82.) In that motion, Watchdog declared that she did not receive Plaintiffs' purported service email, among other grounds for vacatur. (See Doc. No. 82-1 at 3, 8-9, 10, 20; Doc. No. 82-3 at 3.)

On May 24, 2013, almost 100 days after Watchdog denied being served, Plaintiffs moved for a forensic examination purportedly to determine whether this was true. (See Doc. No. 90 at 2.) At this time, Plaintiffs were silent about any plans to use the forensic examination to search for evidence relevant to a separate action pending in the Montgomery County Court of Common Pleas. (See Doc. No. 90.)

On June 5, 2013, Watchdog testified about a computer (the "Target Computer") belonging to her mother, Rose Ann Cantrell, under questioning by Plaintiffs' former counsel:

> Q. Okay. Have you wiped any information from your mom's computer since March of last year?
>
> A. I haven't, but if she has, I don't have control over that.
>
> Q. Okay. To your knowledge, has she wiped any information from her computer since March of last year?
>
> A. I don't think so. I don't know. I don't know.
>
> Q. Do you have any other electronic sources in your house that you use to post information on the web site or to send E-mails, other than your mom's computer?
>
> A. No.
>
> Q. Okay. So if I wanted to look at drafts of postings, would those be on your mom's computer?
>
> A. No.
>
> Q. Are there any records relating to the web site on your mom's computer?
>
> A. No.
>
> Q. There's no records whatsoever?
>
> A. No. I -- I -- at a certain point I stopped making Word documents and putting stuff in and would just post. I wouldn't –
>
> Q. So you would post something on the web site and –
>
> A. Directly on the web site without putting it in a Word document or something like that.

Dep. of Krista C. Brennan 188:4-189:8, June 5, 2013, Cannella v. Resnick Amsterdam Leshner, P.C., No. 2013-02862 (Montgomery Com. Pl. Ct.), excerpt attached hereto as Exhibit B.

Watchdog also testified that she did not have control over any computer used to post on the Truth About Cannella web site. See id. at 187:13.

On June 10, 2013, Watchdog filed papers opposing the forensic examination. (See Doc. No. 94.) Watchdog argued that a court-ordered forensic examination was extreme and invasive, and that she lacked possession, custody, or control over the devices that Plaintiffs were seeking. (See id. at 2, 4-6.)

On June 13, 2013, the Court entered an order granting Plaintiffs' motion for forensic examination. (See Doc. No. 97.) The Court's order provided, in relevant part:

> It is ORDERED that Defendant Watchdog shall, within three days of the date of entry of this Order, identify any and all electronic devices from which she accessed her email accounts truthaboutcannella@yahoo.com and watchdog@truthaboutcannella.net and any documents or records related to the website truthaboutcannella.net. Defendant Watchdog shall then submit these devices and computers for a forensic examination. Defendant Watchdog may select the expert used for the forensic examination, and the Plaintiffs shall pay for the forensic examination.

(Id. at 1-2.) The Court also stayed a motion for discovery that Watchdog had previously filed until she complied with the order. (See id. at 2.)

On the same day that the Court entered its order, Watchdog's counsel contacted IT Acceleration ("ITA"), a company that specializes in digital forensics. (See Doc. No. 112-1 at 3.) Gary Hunt from that firm offered two options: (1) A forensic examiner could come to the home of Watchdog and Ms. Cantrell, whereupon the examiner would disassemble the Target Computer, make a mirror image of the Target Computer's hard drive, and take the image back to ITA's offices; or (2) a device called the "EZ Imager" would be sent to the home of Watchdog and Ms. Cantrell, and one of them could simply connect it to the Target Computer. (See id.) Mr.

Hunt stated that the EZ Imager would automatically copy the Target Computer's hard drive, after which the EZ Imager would be returned to ITA for processing. (See id.) Watchdog's counsel was assured by Mr. Hunt that the EZ Imager was forensically equivalent to the first option. (See id.) Watchdog's counsel asked whether the EZ Imager could be tampered with, and Mr. Hunt said no. (See id.)

On June 14, 2013, Mr. Hunt elaborated on how ITA uses the EZ Imager:

> As we discussed, the EZ Imager is a device that will allow the user to complete the forensic imaging without the need of a forensic technician on-site. The device offers hardware encryption so the data is safe in transit between the user and our office. Once at the office, the forensic bit stream image is transferred to 2 hard drives. This is so in the event of a hard drive failure we will still have access to the image. These hard drives will not leave our locked lab.

(Id. at 15.)

On the next day, Watchdog's counsel emailed this note to Plaintiffs' former counsel and informed him that ITA had been selected for the forensic examination. (See id. at 18-19.) Watchdog's counsel also provided a hyperlink to a video about the EZ Imager. (See id. at 18.) The video provides the following information about the EZ Imager:

> Provides the same results as an onsite collection, but quicker and less costly
>
> Immediately establishes chain-of-custody
>
> Establishes full snapshot, point-in-time preservation of the entire hard drive
>
> Court Compliant
>
> Validated Collection
>
> Legally Defensible

TechTalk – EZ Imager Forensic Collection Appliance with David Yarnall of IT Acceleration, Inc., YouTube (May 25, 2012), http://youtu.be/tc-IEMwI4c8, excerpted screenshots attached hereto as Exhibit C; Second Aff. of Jonathan Z. Cohen ¶ 5, Nov. 8, 2013, attached hereto as Exhibit N.

On June 15, 2013, Watchdog's counsel served Watchdog's Identification of Computers Pursuant to the Court's Order Dated June 13, 2013 ("Watchdog's Identification") on Plaintiffs' counsel. (See Doc. No. 112-1 at 3-4.) Watchdog identified the Target Computer as a computer "from which [she] accessed the email accounts truthaboutcannella@yahoo.com and/or watchdog@truthaboutcannella.net, and/or from which [she] accessed any documents or records related to the web site truthaboutcannella.net." (See Doc. No. 134-1 at 10.) Watchdog did not state that any files relevant to this case remained on the Target Computer. (See id.)

By June 27, 2013, Watchdog's counsel had not received a response to his email to Plaintiffs' former counsel regarding ITA and the EZ Imager. (See Doc. No. 112-1 at 4.) Watchdog's counsel emailed Plaintiffs' former counsel again on that day. (See id.) He wrote: "What is the status of the forensic examination? I ask because the longer this takes, the longer the Court will take to resolve my discovery motion." (Id. at 22.)

On June 28, 2013, Watchdog moved out of her mother's house. See Ex. A at ¶ 8. (See also Doc. No. 112-2 at 3-4.) On that day, Watchdog left the Philadelphia area for Texas. See Ex. A at ¶¶ 8, 9, 11; Second Decl. of Rose Ann Cantrell ¶ 8, Oct. 26, 2013, attached hereto as Exhibit D. Watchdog did not bring the Target Computer with her to Houston; her access to that computer ended when she moved. See Ex. A at ¶ 8; Ex. D at ¶ 8. (See also Doc. No. 112-2 at 4.)

Watchdog's counsel only learned about Watchdog's move on July 7, 2013. (See Doc. No. 112-1 at 7, 31.)

On July 1, 2013, Plaintiffs' newly substituted counsel, Sidney S. Liebesman, emailed Watchdog's counsel, stating that he "would like to discuss the status of the forensic examination." (See id. at 4, 24.) Watchdog's counsel promptly replied: "We served an identification of computers/devices on [Plaintiffs' former counsel] and notified him of our selection of the expert, but have not heard anything since then." (See id. at 4, 29.)

On July 3, 2013, Mr. Liebesman and Watchdog's counsel had a telephone conference regarding the forensic examination. (See id. at 4.) Watchdog's counsel explained the two options given to him by ITA. (See id.) Watchdog's counsel explained that Ms. Cantrell was not his client; that Ms. Cantrell would not speak to him; and that he could not guarantee that Ms. Cantrell would cooperate with a forensic examination. (See id.) Watchdog's counsel stated that he could not guarantee that Ms. Cantrell would welcome strangers in her home, especially for the purpose of disassembling the Target Computer to copy the hard drive. (See id.) Watchdog's counsel conveyed that it was important to "tread lightly." (See id.) The better option, he stated, was to avoid a "scene" at Ms. Cantrell's home by choosing the EZ Imager option. (See id.) Watchdog's counsel told Plaintiffs' counsel that the EZ Imager protocol is forensically sound. (See id. at 5.)

At no time during the July 3, 2013 telephone conference did Watchdog's counsel suggest that he would advise Watchdog to deliberately conceal any copying from her mother. (See id. at 5-6.) In any case, Watchdog had moved out of her mother's house five days earlier. See Ex. A at ¶ 8. (See also Doc. No. 112-2 at 3-4.)

On July 19, 2013, Plaintiffs filed a motion seeking to modify the Court's June 13, 2013 order. (See Doc. No. 107.) Plaintiffs sought leave to serve a subpoena on Watchdog's mother to obtain the Target Computer; to select the forensic examiner; and essentially to seize control over the forensic examination protocol. (See id. at 1-2.) Plaintiffs represented that the scope of the forensic examination would be limited to evidence relevant to this case. (See id. at 1-2, 7-8.) They remained silent about any plans to use the forensic examination to seek evidence related to a Montgomery County action. Finally, Plaintiffs continued to propose that they be responsible for the cost of the forensic examination. (See id. at 1.)

On July 23, 2013, ITA provided additional information about the forensic validity of the EZ Imager:

> The EZ Imager is a hardware encrypted hard drive with a number pad on it. In order to access the drive, the user needs to key in the proper code . . . . It will gather . . . basic chain of custody information from the user. After it has that info, it starts up FTK Imager, an industry accepted forensic imaging tool, and will create a forensic image of the client's hard drive. The forensic image contains all the same data that would be collected through an onsite or in-lab collection effort.

(See id. at 7-8, 35.) ITA also provided a fact sheet about the EZ Imager stating that it is "Legally Defensible" in that the "[c]ollection is authenticated and forensically validated." (See id. at 36.) "Once received, IT Acceleration forensic analysts will authenticate and validate the collection before any work is completed on the data. At this point, the chain of custody is validated and the forensic image authenticated – a legally defensible collection!" (Id.) ITA also revealed that Plaintiffs' counsel had never contacted them. (See id. at 8, 35, 38.)

On August 5, 2013, Watchdog filed papers opposing Plaintiffs' motion to modify the Court's June 13, 2013 order. (See Doc. No. 112.) Watchdog asserted again that she lacked

possession, custody, or control over the Target Computer. (See id. at 2, 3, 14; Doc. No. 112-2 at 3, 4.)

On August 6, 2013, the Court issued an order requiring Ms. Cantrell to produce the Target Computer for forensic examination within 14 days. (See Doc. No. 115.) That order was only entered on the docket and served on counsel three days later. (See id.) Thus, the deadline for complying with the order was functionally shortened by three days. Watchdog's counsel was hospitalized for emergency surgery from August 8 through August 10, 2013, when the Court entered the order. See Ex. N at ¶ 7. After being discharged from the hospital, Watchdog's counsel sent the Court's order to Ms. Cantrell by email, facsimile, and FedEx on August 13, 2013. See Letter from Jonathan Z. Cohen to Rose Ann Cantrell (Aug. 13, 2013), attached hereto as Exhibit O.

On August 14, 2013, after Watchdog's counsel learned that Ms. Cantrell had suffered a heart attack and she might not have received the letter sent the previous day, he sent another letter to her by fax at the Chester County Hospital. See Letter from Jonathan Z. Cohen to Rose Ann Cantrell (Aug. 14, 2013), attached hereto as Exhibit P. Two days later, Ms. Cantrell's son-in-law, David Borda, left a voicemail for Watchdog's counsel, stating: "She is in fact incapacitated and she's more serious than we thought, and will be out of it in the hospital and/or rehab for quite a while—it's a serious heart condition. She's not going to be able to do anything . . . . She's out of it. There's going to be nobody available to do that forensic stuff." Voicemail from David Borda to Jonathan Z. Cohen (Aug. 16, 2013), transcript attached hereto as Exhibit E; Ex. N at ¶ 6. On August 21, 2013, Mr. Borda delivered the Target Computer to ITA. (See Doc. No. 134 at 6.)

On September 13, 2013, Plaintiffs' counsel emailed a list of search terms and "other searches/issues" to ITA and Watchdog's counsel. (See Doc. No. 134-1 at 22-23.) These terms included:

Marion
Babbel
Camacho
CHOP
Jillian
burns
round w/1 3
TAC
Watson
Complaint
Phil
Art
Small
Court
Crash
Scheduled w/1 maintenance
Annuities
Default

(Id.) ITA warned Plaintiffs' counsel that some keyword searches may result in "false positives." See Ex. N at ¶ 8.

On October 2, 2013, Mr. Hunt sent an email to all counsel regarding the forensic examination. Mr. Hunt stated that a program called Tracks Eraser Pro "appears to have been used to delete files." (Id. at 36.) Fragments of data led Mr. Hunt to believe that a user named "Rose" had run Tracks Eraser Pro. (See id.) Mr. Hunt had "no way of confirming what or how much was deleted by" Tracks Eraser Pro. (Id.)

On October 11, 2013, Mr. Hunt executed a declaration regarding the forensic examination. Among other facts, Mr. Hunt declared:

> It was discovered that on July 7, 2013, Windows 7 was reinstalled on the Computer.
> . . . .
> The only user profile on the Computer, "roseanncantrell", was created on July 7, 2013. This account is password protected.
> . . . .
> There are data fragments in the unallocated space indicating the installation of Tracks Eraser Pro and CCleaner.
> . . . .
> The tools Tracks Eraser Pro and CCleaner have functions outside of data wiping related to systems optimization.
> . . . .
> I did not purchase, install, or test Tracks Eraser Pro in my investigation.
> . . . .
> It is not possible to know what data was deleted using Tracks Eraser Pro. The installation date and date of use are also unavailable.
> . . . .
> No investigation was undertaken to determine whether or not the Computer was "hacked."

(Doc. No. 134-1 at 40-41.) Mr. Hunt also stated that the technical support team of Tracks Eraser Pro told him that the presence of certain files on the Target Computer indicates that the program was used. (Id. at 40.)

On the same day, Mr. Hunt sent an email in which he repeated: "I have no way of knowing what it was that [Tracks Eraser Pro] deleted, or how much . . . ." See Email from Gary Hunt to Jonathan Z. Cohen (Oct. 11, 2013), excerpt attached hereto as Exhibit F. In response to questioning by Watchdog's counsel about whether Mr. Hunt actually knew whether Tracks Eraser Pro was used to delete files given the second-hand information that he had received from the program's technical support team, Mr. Hunt stated: "I have attached the email correspondence I have had with Acesoft as a PDF. Taking the statement from AceSoft as fact, the tool was utilized in some way." Id. The "attached" email was from Kevin Liang of Acesoft,

the manufacturer of Tracks Eraser Pro, to Mr. Hunt, dated October 4, 2013. See id. Mr. Liang stated: "it's temp files of tracks erase pro when cleaning hard disk it only contains '00'." Id. Mr. Liang did not state that Tracks Eraser Pro was used to *delete* files. See id.

According to Acesoft, Tracks Eraser Pro has the following features that are not related to deleting files:

> - **Homepage Protection** prevent the websites from modifying your homepage
> - **Boss Key** you can hide the opened browser's windows when other come in

Acesoft, Delete History, http://www.acesoft.net/features.htm (last viewed Nov. 3, 2013), excerpt attached hereto as Exhibit G. The editors of CNET, a popular tech media web site, have complimented the security benefits of Tracks Eraser Pro's erasing tool:

> Erasing your Internet history is important for anyone wishing to keep personal data and private information a secret. Tracks Eraser Pro promises to be a simple, one step way, to keep your history so clean that hackers will have nothing to work with.
> . . . .
> Overall, Tracks Eraser Pro is a great download for people seeking to increase their security and make theft harder for online predators.

Download.com, Tracks Eraser Pro – Free download and software reviews – CNET Download.com, http://download.cnet.com/Tracks-Eraser-Pro/3000-2144_4-10074643.html?tag=rb_content;contentBody (Apr. 20, 2009), excerpt attached hereto as Exhibit H.

The developer of CCleaner describes that program as a "system optimization, privacy and cleaning tool." See Piriform, CCleaner – Features, http://www.piriform.com/ccleaner/features (last viewed Nov. 3, 2013), excerpt attached hereto

as Exhibit I. CCleaner is designed to speed up a computer. See Piriform, CCleaner – CCleaner Optimizes, http://www.piriform.com/ccleaner/features/ccleaner-optimizes (last viewed Nov. 6, 2013), excerpt attached hereto as Exhibit J. This program is popular, and has been favorably reviewed by BBC, the Washington Post, PC World, and the Financial Post. See Piriform, CCleaner – Reviews, http://www.piriform.com/ccleaner/reviews (last viewed Nov. 6, 2013), excerpt attached hereto as Exhibit K.

Watchdog has not deleted any evidence related to this case since at least March 2012. See Ex. A at ¶ 3; Ex. B at 188:5-8. She has no knowledge of anybody else having done so either. See Ex. A at ¶ 4; Ex. B at 188:9-13. Neither Watchdog nor her mother have any knowledge about the alleged Windows 7 reinstallation on July 7, 2013 or any use of CCleaner or Tracks Eraser Pro on the Target Computer. See Ex. A at ¶¶ 16-18; Ex. D at ¶¶ 5-7.

Even before Watchdog moved to Texas, the Target Computer was frequently outside of Watchdog's control. See Ex. A at ¶¶ 5, 6; Ex. D at ¶¶ 12-14. Ms. Cantrell used the Target Computer on many occasions without Watchdog monitoring her activities. See Ex. A at ¶ 5. Likewise, other family members and individuals used the Target Computer on many occasions without Watchdog monitoring their activities. See Ex. A at ¶ 5; Ex. D at ¶¶ 12-14. Watchdog was away from her mother's house—and without access to the Target Computer—in June-July 2012 and December 2012-January 2013, each trip for approximately 4-6 weeks. See Ex. A at ¶ 6. There were also multiple occasions when Watchdog left her mother's home without the Target Computer for several hours at a time. See id.

Since Watchdog appeared in this action, she has filed a great deal of evidence casting doubt on the allegations contained in the FAC. (See generally Doc. No. 82-1, Doc. No. 82-3;

Doc. No. 82-5; Doc. No. 82-6; Doc. No. 116; Doc. No. 117; Doc. No. 132-2.) Plaintiffs have never directly rebutted any of this evidence.

III. LEGAL ARGUMENT

Plaintiffs have failed to meet their high burden to prove that Watchdog spoliated evidence. Even if spoliation occurred, Plaintiffs would suffer little or no prejudice and all of their proposed sanctions would be inappropriate.

A. Plaintiffs Fail to Prove Spoliation.

1. Standard for proving spoliation

"Spoliation occurs where: [1] the evidence was in the party's control; [2] the evidence is relevant to the claims or defenses in the case; [3] there has been actual suppression or withholding of evidence; and [4], the duty to preserve the evidence was reasonably foreseeable to the party." See Bull v. United Parcel Serv., 665 F.3d 68, 73 (3d Cir. 2012) (citing Brewer v. Quaker State Oil Ref. Corp., 72 F.3d 326, 334 (3d Cir. 1995)). A finding of bad faith is essential before a court may sanction a party for spoliation. See id. at 79.

2. Plaintiffs bear a high burden to prove spoliation.

The party alleging spoliation generally bears the burden of proof. See Byrnie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 107–08 (2d Cir. 2001); Stream Cos., Inc. v. Windward Adver., 2013 WL 3761281, *2 (E.D. Pa. July 17, 2013); Tabon v. Univ. of Pa. Health Sys., 2012 WL 2953216, *2 (E.D. Pa. July 20, 2012).

A "clear and convincing evidence" standard for proving spoliation is appropriate, particularly when default judgment or other dispositive sanctions are sought. See Micron Tech., Inc. v. Rambus Inc., 917 F. Supp. 2d 300, 319, 323, 324 (D. Del. 2013); Mahaffey v. Marriott

Int'l, Inc., 898 F. Supp. 2d 54, n. 3 (D.D.C. 2012); Magnetar Techs. Corp. v. Six Flags Theme Park Inc., 886 F. Supp. 2d 466, 481, 489 (D. Del. 2012).[2]

The "clear and convincing" standard "'requires . . . evidence so clear, direct, weighty, and convincing as to enable a clear conviction, without hesitation, about whether or not the defendant[] acted' in a way that renders [her] liable." Kendall v. Daily News Publ'g Co., 716 F.3d 82, 92 (3d Cir. 2013) (quoting Amica Mut. Ins. Co. v. Fogel, 656 F.3d 167, 179 (3d Cir. 2011)).

Accordingly, Plaintiffs bear a high burden to prove that Watchdog spoliated evidence.

3. Much of the evidence sought by Plaintiffs never existed.

Before spoliation of evidence can occur, it is obvious that the evidence must have existed in the first place. Watchdog has claimed for months now that she never received any emails from Plaintiffs' counsel purporting to serve her with process or otherwise providing notice of this suit. (See Doc. No. 82-1 at 5, 10, 20; Doc. No. 82-3 at 3; Doc. No. 116 at 1, 25). If she never received these emails, then they would not be found on the Target Computer. As of June 5, 2013, the Target Computer contained no records related to Watchdog's web site. See Ex. B at 188:19-189:8.

Plaintiffs' assertions that ITA found fragments containing keywords on the Target Computer are insufficient for several reasons. (See Doc. No. 134 at 14.) First, "Cannella," "Watchdog," "Hidemyass," "Alternative Service," "Vorys," and other search terms selected by Plaintiffs appear in filings made in this very action—which are presumably of no interest to

[2] See also Palar v. Blackhawk Bancorporation Inc., 2013 WL 1704302, at *2 (C.D. Ill. Mar. 19, 2013); Makowski v. SmithAmundsen LLC, 2012 WL 3643909, at *3 (N.D. Ill. Aug. 21, 2012); SunTrust Mortg., Inc. v. AIG United Guar. Corp., 2011 WL 1225989, at *20 (E.D. Va. Mar. 29, 2011); Coburn v. PN II, Inc., 2010 WL 3895764, at *3 (D. Nev. Sept. 30, 2010).

Plaintiffs. These filings are precisely the sort of document that an attorney would send to his client. "Cannella" and "Watchdog" appear in these filings too many times to count. "Hidemyass" or variations on that term appear no less than 28 times in such filings.[3] "Alternative Service" or variations on that term appear no less than 54 times.[4] These figures do not account for copies of filings, of course. Likewise, Plaintiffs' keywords appeared in public postings made on Watchdog's web site, which Plaintiffs obviously possess. (See Doc. No. 50-1 at 2-22; Doc. No. 83-1 at 29-37; Doc. No. 87-3.) The mere presence of fragments on the Target Computer containing various keywords does not prove that there was evidence on the Target Computer.

3. Watchdog did not exercise sufficient control over the Target Computer.

Under the Bull spoliation analysis, Plaintiffs must first prove that the evidence that Watchdog allegedly spoliated was within her control. See 665 F.3d at 79. Whether "control" exists is a "very fact specific" question. See Davis v. Gamesa Tech. Corp., 2009 WL 3473391, at *2 (E.D. Pa. Oct. 20, 2009). Courts logically consider whether the evidence was within the alleged spoliator's control *at the time of destruction*. See United States v. Watts, 934 F. Supp. 2d 451, 478 (E.D.N.Y. 2013) (movant for spoliation sanctions must prove "that the opposing party had control over the evidence and an obligation to preserve it at the time it was destroyed"); Magnetar, 882 F. Supp. 2d at 490 ("the documents were clearly under the control of [alleged spoliator] at the time of their destruction"); Harkabi v. SanDisk Corp., 275 F.R.D. 414, 418 (S.D.N.Y. 2010) (same as Watts, 934 F. Supp. 2d at 478).

[3] (See Doc. No. 84 at 5, 7, 53; Doc. No. 87 at 2, 3; Doc. No. 87-1 at 3, 8; Doc. No. 87-3 at 2; Doc. No. 116 at 5, 6, 47.)

[4] (See Doc. No. 13 at 1, 4; Doc. No. 17 at 1, 2; Doc. No. 48 at 1, 2; Doc. No. 50 at 4, 7; Doc. No. 82-2 at 2; Doc. No. 83 at 10, 12; Doc. No. 83-1 at 1, 5, 8, 9; Doc. No. 83-2 at 1, 4, 5; Doc. No. 84 at 13; Doc. No. 87 at 4; Doc. No. 88; Doc. No. 91 at 5, 8; Doc. No. 94 at 8; Doc. No. 110 at 2, 3, 7; Doc. No. 116 at 7.)

Whether the alleged spoliator's control is exclusive is also considered in the spoliation analysis. See Patel v. Havana Bar, Rest. & Catering, 2011 WL 6029983, at *9 (E.D. Pa. Dec. 5, 2011) ("spoliation inference is appropriate because the video footage was within [defendant's] exclusive control"); Kvitka v. Puffin Co., L.L.C., 2009 WL 385582, at *7 (M.D. Pa. Feb. 13, 2009) (spoliation elements satisfied as laptop was within plaintiffs' exclusive control); Paramount Pictures Corp. v. Davis, 234 F.R.D. 102, 112 (E.D. Pa. 2005) (spoliation inference appropriate when "information stored on the computer was within defendant's exclusive control").

The Target Computer was frequently outside of Watchdog's exclusive control. The Target Computer belongs to Watchdog's mother. (See Doc. No. 94-1 at 2; Doc. No. 112-2 at 2, 3, 4). Ms. Cantrell's ownership of the Target Computer is a fact that appears repeatedly in Plaintiffs' motion papers. (See Doc. 134 at 6, 9, 11; Doc. No. 134-1 at 18, 38). While Watchdog used the Target Computer before departing her mother's home, she frequently lacked exclusive control over it. See Ex. A at ¶¶ 5, 6; Ex. D at ¶¶ 12-14. Ms. Cantrell, other family members, and even an independent contractor accessed the Target Computer at various times. See Ex. A at ¶ 5; Ex. D at ¶¶ 12-14. Watchdog was away from the Target Computer on many occasions, including during several extended trips out of state. See Ex. A at ¶ 6.

Whatever non-exclusive control Watchdog exercised over the Target Computer departed entirely as she departed her mother's house on June 28, 2013. On that day, Watchdog left the Philadelphia area for Houston, Texas. See id. at ¶¶ 6-12; Ex. D at ¶ 9. She did not take the Target Computer with her. See Ex. A at ¶ 8; Ex. D at ¶¶ 8, 9. On July 7, when Plaintiffs allege that the

spoliation occurred, Watchdog was more than 1,300 miles away. See Ex. A at ¶¶ 14, 16; Ex. D at ¶¶ 8, 9.

Accordingly, Plaintiffs fail prove that Watchdog had sufficient control over the Target Computer.

4. If there was any evidence on the Target Computer, Plaintiffs have not proven its relevance.

The second element in proving spoliation is a showing that the evidence is relevant to the claims or defenses in the case. See Bull, 665 F.3d at 73. Plaintiffs must "'come forward with plausible, concrete suggestions as to what the [lost] evidence might have been.'" See Centimark Corp. v. Pegnato & Pegnato Roof Mgmt., Inc., 2008 WL 1995305, at *7 (M.D. Pa. May 6, 2008) (quoting Schmid v. Milwaukee Elec. Tool Corp., 13 F.3d 76, 80 (3d Cir. 1994)). The movant should offer some indication as to the likely substance of the lost evidence, including that the evidence would favor the movant. See Chen v. District of Columbia, 839 F. Supp. 2d 7, 14 (D.D.C. 2011); Skeete v. McKinsey & Co., Inc., 1993 WL 256659, at *7 (S.D.N.Y. July 7, 1993); Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 76-77 (S.D.N.Y. 1991).

Plaintiffs' offering of partial bits of data allegedly containing certain keywords is inadequate to show relevance. First, Plaintiffs have not come forward with any "plausible, concrete suggestions as to what the [lost] evidence might have been," let alone any indication that the evidence would favor Plaintiffs. See Chen, 839 F. Supp. 2d at 14; Centimark, 2008 WL 1995305 at *7; Skeete, 1993 WL 256659 at *7; Turner, 142 F.R.D. at 76-77. We are left to merely speculate.

Second, as discussed above, there is no indication of the extent to which Plaintiffs' keywords appeared in files other than filings made in this very case or in postings from Watchdog's web site.

Third, many of the keywords appear to have nothing to do with this case:

> Felder
> McWilliams
> Resnick
> A technical glitch
> charlemagneoebjcf@gmail.com
> kristabrennan.grrl@gmail.com
> McCaffery
> RBC
> Granite Financial
> Guyton
> Senior Safety Net
> Another character killing moment
> Marion
> Babbel
> Camacho
> CHOP
> LPL Financial
> jillian
> burns
> round w/1 3

(See Doc. No. 9; Doc. No. 134-1 at 33-34.) Plaintiffs essentially admit that one purpose of their forensic examination was to fish for evidence related to another case pending in the Montgomery County Court of Common Pleas. (See Doc. No. 134 at 6.)[5]

[5] Watchdog anticipates that Plaintiffs will argue that the two actions are intimately related. By Plaintiffs' own admission, however, the two cases are "drastically different." See Pls.' Mem. of Law Opp'n to Def. Arthur Felderstein's Prelim. Objections 5, Apr. 8, 2013, Cannella v. Amsterdam Resnick Leshner, P.C., No. 2013-02862 (Montgomery Com. Pl. Ct.), excerpt attached hereto as Exhibit M.

Fourth, some of the keywords that Plaintiffs selected are relevant but likely to have resulted in "false positives" because they are common terms or phrases; they are parts of common terms or phrases; or they are likely to appear in contexts other than this case:

TAC
Watson
Complaint
Phil
Art
Small
Court
Crash
Scheduled w/1 maintenance
Annuities
Default[6]

(See Doc. No. 134-1 at 33-34.) As ITA warned Plaintiffs' counsel, "false positives" can be a concern with keyword searches in forensic examinations. Cf. Rhoads Indus., Inc. v. Building Materials Corp. of Am., 254 F.R.D. 216, 220 (E.D. Pa. 2008) ("Keyword and name searches are frequently employed as an initial method to screen and sort documents, but they are not foolproof."); Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 257, 261 (D. Md. 2008) ("Common sense suggests that even a properly designed and executed keyword search may prove to be over-inclusive or under-inclusive . . ."). To offer an example of how a seemingly distinctive word can result in false positives, ITA reported that the word "Joyner" appeared in an electronic dictionary on the Target Computer.

Accordingly, Plaintiffs have not met the relevance requirement in proving spoliation.

[6] "Default" is an especially poor keyword for a computer forensic examination given one of its definitions: "a selection automatically used by a computer program in the absence of a choice made by the user." See Default Definition, Merriam-Webster, http://www.merriam-webster.com/dictionary/default (last viewed Nov. 6, 2013).

5. Watchdog has not suppressed or withheld evidence.

The third element in proving spoliation is that "there has been actual suppression or withholding of evidence." See Bull, 665 F.3d at 79. "No unfavorable inference arises when the circumstances indicate that the document or article in question has been lost or accidentally destroyed, or where the failure to produce it is otherwise properly accounted for." Brewer, 72 F.3d at 334. The Third Circuit has recently held that "bad faith is pivotal to a spoliation determination." See Bull, 665 F.3d at 79; Bozic v. City of Washington, 912 F. Supp. 2d 257, 268-69 (W.D. Pa. 2012). See also In re Adams Golf, Inc., Secs. Litig., 618 F. Supp. 2d 343, 351 (D. Del. 2013) ("party charging spoliation must prove that there was an intentional destruction of documents"). In the spoliation context, "bad faith" means that the alleged spoliator "'intended to impair the ability of the potential defendant to defend itself.'" See Micron, 917 F. Supp. 2d at 315 (quoting Schmid, 13 F.3d at 80); Magnetar, 886 F. Supp. 2d at 481 (same).

Plaintiffs' assertions that Watchdog suppressed evidence are easily overcome. First, as discussed above, Plaintiffs have not proven that there was evidence to suppress on the Target Computer in the first place. Second, assuming that there was evidence on the Target Computer, Plaintiffs offer no evidence that it was deleted in the way that they allege. Mr. Hunt's statements that Tracks Eraser Pro was used are hearsay. See F.R.E. 801, 802. Mr. Hunt did not test Tracks Eraser Pro, and his statement that this program was used is based on the cryptic statements of somebody else. (See Doc. No. 134-1 at 40, 41.)[7] See also Ex. F. Even if Tracks Eraser Pro was used, that fact alone would be insufficient to show that it was used to delete data, as Tracks Eraser Pro has uses other than deletion. (See Doc. No. 134-1 at 41.) See also Ex. G. And even if

[7] Prior to executing his declaration, Mr. Hunt hedged on this point: "Tracks Eraser Pro *appears* to have been used to delete files." (See Doc. No. 134-1 at 36.) (emphasis added).

Tracks Eraser Pro was used to delete data, such an act would not be inherently suspect; erasing data can actually improve computer security. See Ex. H. Further still: If Tracks Eraser Pro was used to delete data, Plaintiffs offer no evidence that it was used to delete evidence related to this case. Mr. Hunt clearly stated:

> I currently have no way of confirming what or how much was deleted by the software.
>
> It is not possible to know what data was deleted using Tracks Eraser Pro.

(Doc. No. 134-1 at 36, 41). Plaintiffs likewise offer no evidence that CCleaner was used to delete data or that the reinstallation of Windows 7 resulted in deletion.[8]

Third, assuming that evidence once resided on the Target Computer and was subsequently deleted, Plaintiffs offer no evidence that *Watchdog* deleted it. Watchdog was in Texas on July 7, 2013, the date that Plaintiffs allege that spoliation occurred. See Ex. A at ¶¶ 14, 16; Ex. D at ¶ 9.[9] Watchdog did not ask her mother or anybody else to delete evidence. See Ex. A at ¶¶ 4, 16-18; Ex. D at ¶ 11.

---

[8] The uncertainties in Mr. Hunt's declaration are only multiplied in the declaration of Plaintiffs' expert, John B. McElhatton. Mr. McElhatton's declaration is based on a telephone conversation with Mr. Hunt and an examination of Mr. Hunt's declaration. (See Doc. No. 134-1 at 26.) In that respect, Mr. McElhatton's declaration is hearsay. See F.R.E. 801, 802. Mr. McElhatton's declaration also provides a perfect example of the pitfalls of relying on hearsay evidence: He states a "belief that someone took great pains to render certain data irrecoverable on the examined system. The first line of defense was to encrypt the data . . ." (Doc. No. 134-1 at 30.) But eight days after Mr. McElhatton executed his declaration, ITA retracted their finding that the Target Computer was encrypted in any way. (See Doc. No. 135-2.) Lastly, Mr. McElhatton's declaration is not compliant with 28 U.S.C. § 1746; it is not made under penalty of perjury (nor could it be given his lack of first-hand knowledge about the Target Computer). (See Doc. No. 134-1 at 30.)

[9] Even if Watchdog was sitting in front of the Target Computer in West Chester—instead of 1,300 miles away—Plaintiffs could not meet their high burden by coupling Watchdog's IT background with Mr. McElhatton's opinion that reinstalling Windows 7 requires a "fair amount of technical expertise." (See Doc. No. 134 at 15; Doc. No. 134-1 at 29). By simply searching Google for "How do I reinstall Windows 7," a novice can learn how to do just that. See Google, How do I reinstall Windows 7 - Google Search, https://www.google.com (type "How do I reinstall Windows 7"; click "Google Search"), attached hereto as Exhibit L.

Finally, assuming that Watchdog deleted evidence on the Target Computer, Plaintiffs offer no evidence of the required bad faith. See Bull, 665 F.3d at 79; Bozic, 912 F. Supp. 2d at 268-69. Files may be placed in a hard drive's unallocated space by a program or by an operating system—not necessarily by the computer user. See Ex. F ("A file's presence in the unallocated means it was deleted either by the system or the user."). Plaintiffs' expert suggests the same:

> Unallocated file space potentially contains intact files, remnants of files and subdirectories and temporary files which were transparently created and deleted by *computer applications and/or the operating system* . . . . One example of how this ambient data occurs is when a program is *writing data to a disc and the computer system crashes or is turned off before the file could be closed. The data is still on the disk, but the directory entry was not updated. The data is written to unallocated space.*

(Doc. No. 134-1 at 28.) (emphasis added). Even when files are intentionally deleted, this does not mean that they were *volitionally* deleted. See Coburn, 2010 WL 3895764 at *5. In other words, an individual may intentionally command a computer program to do something without understanding the potential for data deletion. See id.

Accordingly, Plaintiffs have not met their burden to show that Watchdog suppressed or withheld evidence.

6. Plaintiffs fail to show a reasonably foreseeable duty to preserve any evidence on the Target Computer.

The final element required to prove spoliation is that "the duty to preserve the evidence was reasonably foreseeable to the party." See Bull, 665 F.3d at 73. A party need not preserve every document in her possession—only those "reasonably related to foreseeable litigation." See Haskins v. First Am. Title Ins. Co., 2012 WL 5183908, at *4 (D.N.J. Oct. 18, 2012). "When litigation is reasonably foreseeable is a flexible fact-specific standard that allows a district court to

exercise the discretion necessary to confront the myriad factual situations inherent in the spoliation inquiry." Anderson v. Sullivan, 2013 WL 4455602, at *4 (W.D. Pa. Aug. 16, 2013) (citing Bull, 665 F.3d at 77-78)).

A simple review of salient dates shows that Plaintiffs have not carefully analyzed the last element of the spoliation test: Watchdog created the truthaboutcannella.com web site on January 17, 2011. (Doc. No. 82-3 at 2.) She created the truthaboutcannella.net web site on March 10, 2011. (Id.) This lawsuit was filed on March 9, 2012. (See Doc. No. 1). The FAC, containing new claims, was filed on July 31, 2012. (See Doc. No. 9.) Plaintiffs claim to have served Watchdog by email on August 30, 2012, but she did not receive it. See Ex. A at ¶ 3. (See also Doc. No. 82-3 at 3.) Watchdog first learned of this lawsuit in mid-December 2012. See Ex. A at ¶ 3. (See also Doc. No. 82-3 at 4.) Thus, Watchdog could have deleted files relevant to this matter between January 17, 2011 and mid-December 2012 without any liability. Even if Watchdog knew that this case had been filed on March 9, 2012 (Doc. No. 1), there would still be a large block of time in which she could have legitimately deleted files.

Plaintiffs have offered no evidence that any data deletion occurred after litigation became reasonably foreseeable to Watchdog. Even assuming that Watchdog deleted relevant evidence using Tracks Eraser Pro, the date that this program was used is unknown. (See Doc. No. 134-1 at 41.) And assuming that the reinstallation of Windows 7 on July 7, 2013 resulted in the deletion of relevant evidence, there is no evidence that Watchdog did this—only evidence that she was in Texas at the time. See Ex. A at ¶¶ 14, 16; Ex. D at ¶ 9.

Accordingly, Plaintiffs have not met their burden to show a reasonably foreseeable duty to preserve evidence. See Bull, 665 F.3d at 73.

B. Even Assuming that Spoliation Occurred, Plaintiffs Would Suffer Little or no Prejudice.

Upon a finding that spoliation occurred, the court must consider "the degree of prejudice suffered by the opposing party." See Bull, 665 F.3d at n. 5 (quoting Schmid, 13 F.3d at 79). Prejudice requires proof that the spoliation "'materially affect[ed] the substantial rights of the adverse party and is prejudicial to the presentation of his case.'" Magnetar, 886 F. Supp. 2d at 481 (quotation omitted). The movant must "'come forward with plausible, concrete suggestions as to what the evidence might have been.'" Id. (quoting Schmid, 13 F.3d at 80)). More is required than "a fertile imagination that access to the [lost documents] would have produced evidence favorable to [the movant's] cause.'" See Adams Golf, 618 F. Supp. 2d at 352 (quotation omitted). Furthermore, "[w]hen considering the degree of prejudice suffered by the party that did not destroy the evidence, the court should take into account whether that party had a meaningful opportunity to examine the evidence in question before it was destroyed." AMG Nat'l Trust Bank v. Ries, 2011 WL 3099629, at *5 (E.D. Pa. July 22, 2011) (Joyner, J.) (quoting Davis, 234 F.R.D. at 112).

Plaintiffs' bare assertions of prejudice fail for a number of reasons: First, whether Watchdog received Plaintiffs' purported service emails remains irrelevant because the summons purportedly emailed by Plaintiffs' counsel was defective; Plaintiffs had no right to file their FAC; and Watchdog would not have been required to respond to that pleading even if it had been properly filed. (See Doc. No. 82-1 at 9-13; Doc. No. 116 at 8-10; Doc. No. 108-1 at 2-5.) Watchdog incorporates by reference the above-cited portions of her Brief in Support of Motion to Vacate Default and Default Judgment, Reply and Supplemental Points in Support of

Defendant Watchdog's Motion to Vacate Default and Default Judgment, and Defendant Watchdog's Motion to Dismiss Plaintiffs' Verified First Amended Complaint.

Second, assuming that any spoliation, sanctions would not be warranted because the parties have not determined whether any copies of the allegedly deleted data exist. Watchdog continues to investigate this. In the event that Watchdog discovers any backup copies of the allegedly deleted data, then Plaintiffs will have suffered no prejudice. Plaintiffs' motion for sanctions is premature at best.

Third, even Plaintiffs are not entirely convinced that the Target Computer's hard drive is useless. In their own words: "Plaintiffs need the copy of the mirror image for the continued prosecution of this action and the action . . . to the extent that the bits of data in the unallocated space provide additional information." (Doc. No. 134 at 26.) This begs the question of whether Plaintiffs should have reviewed the data prior to filing their motion for sanctions.

Fourth, few if any of Plaintiffs' allegations in this case ride on the contents of the Target Computer—and Plaintiffs do not suggest otherwise in their motion. Truth is a defense to defamation, tortious interference with business relations, and civil conspiracy arising out of defamation or tortious interference. See Pacitti v. Durr, 310 Fed. Appx. 526, 528 (3d Cir. Feb. 11, 2009) (defamation); Feldman & Pinto, P.C. v. Seithel, 2011 U.S. Dist. LEXIS 147655, at *22 (E.D. Pa. Dec. 22, 2011) (tortious interference with business relations); Rock v. Rangos, 2013 PA Super 13, 61 A.3d 239, 249 (Pa. Super. Ct. 2013) ("conspiracy claim will not lie without a valid underlying civil claim"). Plaintiffs are in the best position to have evidence regarding whether these claims are true. The remaining claim, for violations of the Lanham Act—and the only claim providing federal subject-matter jurisdiction over this case—has been doomed from the

beginning given that Watchdog was not in competition with Plaintiffs. (See Doc. No. 82-1 at 16-17 (citing Nevyas v. Morgan, 309 F. Supp. 2d 673, 680 (E.D. Pa. 2004)); Doc. No. 82-3 at 5.)

Finally, assuming that any spoliation occurred and that Watchdog is responsible, Plaintiffs were not diligent in seeking the forensic examination. Since February 15, 2013, Watchdog has denied receiving the service emails purportedly sent by Plaintiffs' counsel. (See Doc. No. 82 at 5, 8-9, 20; Doc. No. 82-3 at 3.) However, Plaintiffs waited until May 24, 2013—nearly 100 days—to seek a forensic examination. (See Doc. No. 90.) Having retained Mr. Anderson, Plaintiffs were well-aware of the benefits of a forensic examination. (See Doc. No. 90-1.) Even after the Court ordered the forensic examination, Plaintiffs continued to waste repeated opportunities to examine the Target Computer before July 7, 2013. (See Doc. No. 112-1 at 3-5, 7, 8, 18, 22, 24, 29, 35, 38.)[10]

Accordingly, Plaintiffs have suffered little no prejudice.

C. Assuming that Spoliation Occurred, None of the Sanctions Proposed by Plaintiffs Would be Appropriate.

Upon finding that a party has spoliated evidence, the court must consider "whether there is a lesser sanction that will avoid substantial unfairness to the opposing party." See Bull, 665 F.3d at n. 5 (quoting Schmid, 13 F.3d at 79). Plaintiffs propose the following sanctions: (1) that Watchdog be held in contempt of the Court's June 13, 2013 order; (2) that the Court impose sanctions under Federal Rule of Civil Procedure 37; (3) that Watchdog's Motion to Vacate Default and Default Judgment be denied; (4) that the Court make an adverse inference that

[10] Watchdog anticipates that Plaintiffs will argue that using the EZ Imager would not have been a "meaningful opportunity to examine the evidence." See Ries, 2011 WL 3099629 at *5. Such an argument would fail because the EZ Imager is forensically equivalent to an in-person data collection. (See Doc. No. 112-1 at 3, 7-8, 15, 35, 36.) See also Ex. C.

Watchdog received service of process and had notice of this action; (5) that Watchdog be held solely responsible for all fees and costs associated with ITA's work; (6) that Watchdog pay for Plaintiffs' attorneys' fees and costs; and (7) that ITA provide a copy of the mirror image of the Target Computer to Plaintiffs' counsel. (See Doc. No. 134 at 1-2.) Given that Watchdog did not spoliate evidence, none of these sanctions are appropriate. Nonetheless, Watchdog offers observations below about why each sanction proposed by Plaintiffs would be inappropriate even in the unlikely event that Plaintiffs prove spoliation.

(a) *Contempt of Court's June 13, 2013 order*

Plaintiffs request that Watchdog be held in contempt of the Court's June 13, 2013 order. (See Doc. No. 134 at 1.) "The plaintiff has a heavy burden to show a defendant guilty of civil contempt. It must be done by 'clear and convincing evidence,' and where there is ground to doubt the wrongfulness of the conduct, he should not be adjudged in contempt." Robin Woods Inc. v. Woods, 28 F.3d 396, 399 (3d Cir. 1994) (quoting Quinter v. Volkswagen of Am., 676 F.2d 969, 974 (3d Cir.1982)). Watchdog has several meritorious defenses to contempt:

First, an actual violation of a court order is a prerequisite to contempt. See Roe v. Operation Rescue, 54 F.3d 133, 137 (3d Cir. 1995). Further, "there is a 'longstanding salutary rule in contempt cases that ambiguities and omissions in orders redound to the benefit of the person charged with the contempt.'" Woods, 28 F.3d at 399 (quotation omitted). Plaintiffs suggest that Watchdog violated the Court's June 13, 2013 order by not "submitting" the Target Computer for forensic examination. (See Doc. No. 134 at 6, 11.) But a well-known definition of "submit" is to "subject to a condition, treatment, or operation." See Submit Definition, Merriam-Webster, http://www.merriam-webster.com/dictionary/submit (last viewed Nov. 5,

2013). By offering to image the Target Computer with the EZ Imager, Watchdog complied with the order. Even if Watchdog misinterpreted the order, the meaning of "submit" in this context would be an ambiguity that must be construed in her favor. See Woods, 28 F.3d at 399. Whatever the Court meant by the word "submit," the order does not state exactly when the "submission" must be effectuated—unlike the certain deadline provided in the previous sentence. (See Doc. No. 97 at 1.) Again, this ambiguity must be construed in Watchdog's favor. See Woods, 28 F.3d at 399.

Second, a party cannot be held in contempt if she "substantially complied" with a court order or if she took reasonable steps to comply. See Harris v. City of Phila., 47 F.3d 1311, 1324 (3d Cir. 1995); Halderman v. Pennhurst State Sch. & Hosp., 154 F.R.D. 594, 608 (E.D. Pa. 1994). Watchdog asked her mother whether she could produce the Target Computer to ITA; her mother said no. See Ex. A at ¶ 19 (See Doc. No. 94-1 at 2.) Accordingly, Watchdog substantially complied with the Court's June 13, 2013 order.

To the extent that Plaintiffs suggest that spoliation violates the Court's order, (see Doc. No. 134 at 16), they are wrong. The order is silent about spoliation. (See Doc. No. 97.) Obviously Watchdog understands that there is an independent duty not to spoliate evidence regardless of the contents of any court order. Nonetheless, for the purpose of proving contempt, there must be an unambiguous violation of a court order. See Roe, 54 F.3d at 137; Woods, 28 F.3d at 399.

Accordingly, contempt would not be an appropriate sanction.

(b) *Sanctions under Rule 37*

Plaintiffs suggest that Watchdog should be sanctioned under Federal Rule of Civil Procedure 37. (See Doc. No. 134 at 16, 23, 24.) Specifically, Plaintiffs request that the Court

sanction Watchdog "for spoliating evidence and violating the June 13 Order pursuant to Fed. R. Civ. P. 37(b)(2)(A) and 37(b)(2)(C)." (Id. at 28.) Rule 37 sanctions in the context of spoliation require clear and convincing evidence. See Coburn, 2010 WL 3895764 at *3 (citing 7–37A James Wm. Moore et al., Moore's Federal Practice § 37A.55).

Plaintiffs' assertions on Rule 37 are unfounded. First, while Watchdog certainly recognizes an independent duty to not spoliate evidence, Rule 37's terms do not prohibit spoliation. See Fed. R. Civ. P. 37. Therefore, Rule 37 does not apply to Plaintiffs' motion. Cf. Black Horse Lane Assocs., L.P. v. Dow Chem. Corp., 228 F.3d 275, 302 (3d Cir. 2000) ("unlike subdivision (b) of Rule 37, on its face subdivision (d) does not require the court, prior to imposing sanctions, to have issued an order compelling discovery."); Aguilar v. WEI Equip., 2003 WL 22120268, at *3 (E.D. Pa. Sept. 9, 2003) ("the array of Rule 37(b) sanctions is triggered only when a properly recorded discovery order is violated").

Second, even if Watchdog violated the Court's June 13, 2013 order by not "submitting" the Target Computer for forensic examination, she would have been "substantially justified" under Rule 37(b)(2)(C) under the same defenses that Watchdog raised against contempt. (See Doc. No. 94-1 at 2; Doc. No. 112-2 at 3; Doc. No. 112-4 at 7-8.)

According, Rule 37 sanctions would be inappropriate.

(c) *Denial of Watchdog's Motion to Vacate Default and Default Judgment*

Plaintiffs ask the Court to deny Watchdog's Motion to Vacate Default and Default Judgment as a sanction for spoliation. (See Doc. No. 134 at 4, 25.) "Default judgment is one of the most drastic sanctions 'because [it] strike[s] at the core of the underlying lawsuit.'" TelQuest Int'l Corp. v. Dedicated Bus. Sys., Inc., 2009 WL 690996, at *3 (D.N.J. Mar. 11, 2009)

(quotation omitted). It should be considered only as a "'last resort,' to be imposed only if no alternative remedy by way of a lesser, but equally efficient sanction is available." Motown Record Co. v. DePietro, 2007 WL 1725604, at n.1 (E.D. Pa. June 11, 2007) (quotation omitted).

Before imposing dispositive sanctions for spoliation, the court must find the evidence clear and convincing. See Micron, 917 F. Supp. 2d at 319, 323, 324 (dismissal); Mahaffey, 898 F. Supp. 2d at n. 3 (default judgment); Hynix Semiconductor Inc. v. Rambus Inc., 897 F. Supp. 2d 939, 978 (N.D. Cal. 2012); Magnetar, 886 F. Supp. 2d at 481, 489 (judgment or dismissal). Plaintiffs have not remotely proven that Watchdog spoliated evidence by clear and convincing evidence. To the contrary, the evidence is clear that Watchdog was in Texas when the alleged spoliation occurred. See Ex. A at ¶¶ 8-14; Ex. D at ¶¶ 8, 9.

Accordingly, denial of Watchdog's Motion to Vacate Default and Default Judgment would be inappropriate.

(d) *Adverse inference that Ms. Brennan received service and notice of this action*

Plaintiffs request an adverse inference that Ms. Brennan "received service of process by email on August 30, 2012 and had the appropriate notice of this litigation." (See Doc. No. 134 at 1, 25.) The test for determining whether an adverse inference for spoliation is appropriate is essentially the same as the test for spoliation generally. Compare Bull, 665 F.3d at 73, with Davis, 234 F.R.D. at 112. Given that Plaintiffs have failed to prove spoliation, they are not entitled to a spoliation inference.

Even if a spoliation inference would be appropriate in this case, Plaintiffs' requested inference would be inappropriate. First, this inference would not make sense at trial, when the merits of the case will be decided. Second, Plaintiffs' proposed adverse inference is mandatory as

opposed to permissive. (See Doc. No. 134 at 1, 25.) Spoliation inferences typically involve an instruction that the jury *may* infer that certain spoliated evidence would be unfavorable to the spoliator. See Ries, 2011 WL 3099629 at *5; Mosaid Techs. Inc. v. Samsung Elecs. Co., Ltd., 348 F. Supp. 2d 332, 336 (D.N.J. 2004). Mandatory spoliation inferences are exceptional. See Beck v. Test Masters Educ. Servs., Inc., 289 F.R.D. 374, 380 (D.D.C. 2013) (citing cases).

Accordingly, Plaintiffs' request for an adverse inference is inappropriate.

(e) *Responsibility for the costs of ITA*

Plaintiffs ask the Court to order Watchdog to pay for all costs charged by ITA. (See Doc. No. 134 at 1-2, 25.) This sanction would be inappropriate for several reasons. First, only Plaintiffs sought this forensic examination; Watchdog vigorously opposed it at all times. (See Doc. No. 90; Doc. No. 94; Doc. No. 111; Doc. No. 112.) Watchdog argued that a court-mandated forensic examination was extreme and invasive. (See Doc. No. 94 at 4-5.)

Second, the Court required Plaintiffs to pay for the forensic examination. (See Doc. No. 97 at 2.) There is no indication from the Court's order that responsibility for paying for the forensic examination would ultimately depend on the results of the examination. (See id.)

Third, Watchdog never led Plaintiffs to believe that relevant evidence would be found on the Target Computer. Watchdog actually testified that relevant records would *not* be found on the Target Computer. See Ex. B at 188:19-189:8.[11] If Plaintiffs still expected to find evidence on the Target Computer, then they failed to heed the evidence before them.

[11] Watchdog anticipates that Plaintiffs will argue that her identification of the Target Computer in response to the Court's June 13, 2013 order led them to believe that evidence would be found there. To be clear, the Court ordered Watchdog to "identify any and all electronic devices from which she accessed . . . any documents or records related to the website truthaboutcannella.net"—at Plaintiffs' request—and Watchdog did just that. (See Doc. No. 97 at 1; Doc. No. 134-1 at 10-12.) The fact that Watchdog accessed documents related to truthaboutcannella.net on the Target Computer at some unspecified point in the past does not mean that such documents remained accessible on the Target Computer at the time that she made the identification.

Fourth, Watchdog did her best to effectuate the forensic examination prior to July 7, 2013—when Plaintiffs allege that the spoliation occurred. Watchdog's counsel repeatedly attempted to effectuate the imaging of the Target Computer between June 15, 2013 and July 7, 2013, but received no cooperation from Plaintiffs' counsel. (See Doc. No. 112-1 at 3-4, 7, 8, 15, 18-19, 22, 24, 29, 35, 38.) By proposing the EZ Imager option, Watchdog's counsel even attempted to save Plaintiffs money. (See id. at 18.) If Plaintiffs had cooperated, they would likely have obtained an image of the Target Computer's hard drive before July 7, 2013—and at a lower price.

Finally, Watchdog should not have to cover the forensic examination given that a substantial purpose of it was to collect evidence for a "drastically different" action to which she is not a party. Plaintiffs state in their motion:

> Brennan's spoliation causes incalculable prejudice not only with respect to both the motion to vacate and the ultimate merits in this case, but also to a related case pending in the Montgomery County Court of Common Pleas.
> . . . .
> Plaintiffs need the copy of the mirror image for the continued prosecution of this action and the action pending in the Montgomery County Court of Common Pleas . . . .

(Doc. No. 134 at 6, 26.) See also Ex. M at 5. Plaintiffs' irrelevant keyword selections confirm the dual purpose of the examination. (See Doc. No. 134-1 at 22-23). Watchdog should not have to pay for Plaintiffs' undisclosed, unauthorized fishing expedition.

Accordingly, Watchdog should not be held responsible for the costs of the forensic examination.

(f) *Fees and costs of Plaintiffs' attorneys and expert*

Plaintiffs request that Watchdog pay for all of their fees and costs associated with opposing her motion to vacate default judgment, their motion to modify the June 13, 2013 order, their motion for sanctions, and their fees and costs for hiring a computer expert. (See Doc. No. 134 at 2, 26.) Plaintiffs do not indicate whether such fees or costs should be awarded under a rule, statute, or the Court's inherent power. The only rule that Plaintiffs mention that references attorneys' fees is Rule 37, which does not apply here for the reasons discussed above.

Before imposing sanctions under the Court's inherent power, the Court must find bad faith conduct. See Fellheimer, Eichen & Braverman, P.C. v. Charter Techs., Inc., 57 F.3d 1215, 1225, 1227 (3d Cir. 1995); Spencer v. Steinman, 1999 WL 33957391, at *1 (E.D. Pa. Feb. 26, 1999). Bad faith must be proven by clear and convincing evidence. See Ali v. Tolbert, 636 F.3d 622, 627 (D.C. Cir. 2011); Shepherd v. Am. Broad. Cos., Inc., 62 F.3d 1469, 1477 (D.C. Cir. 1995). In exercising inherent power, the Court should act with restraint, recognizing that "the standards for bad faith are necessarily stringent." See Press v. McNeal, 568 F. Supp. 256, 258 (E.D. Pa. 1983) (citing Roadway Express, Inc. v. Piper, 447 U.S. 752, 764 (1980)).

"Attorneys' fees are generally awarded only in 'narrowly defined circumstances, such as a sanction . . . where a party has 'acted in bad faith, vexatiously, wantonly, or for oppressive reasons.'" Int'l Plastics & Equip. Corp. v. Taylor's Indus. Servs., LLC, 2011 WL 1399081, at *6 (W.D. Pa. Apr. 12, 2011) (quotations omitted). The party seeking attorneys' fees must prove that the fees are reasonable. Lewis v. Mazda Motor of Am., Inc., 2012 WL 6634145, at *2 (D.V.I. Dec. 20, 2012). Monetary sanctions should "relate directly" to the offending party's misconduct. Cf. Barkouras v. Hecker, 2007 WL 777664, at *7 (D.N.J. Mar. 12, 2007) (in context of Rule 16(f) and

37(b) sanctions). In the spoliation context, monetary sanctions are appropriate to "'compensate a party for the time and effort it was forced to expend in an effort to obtain discovery' to which it was otherwise entitled" or for expenses that are a "direct result" of the spoliation. Stream, 2013 WL 3761281 at *6 (quoting Mosaid, 348 F. Supp. 2d at 339).

Even in the unlikely event that Plaintiffs' prove spoliation, their request for fees and costs would be greedy and unwarranted. With the exception of Plaintiffs' opposition to Watchdog's motion to vacate (Doc. No. 82; Doc. No. 87), all of the fees and costs that Plaintiffs seek to shift are tainted by Plaintiffs' unauthorized discovery for the Montgomery County action. Plaintiffs wanted to "kill two birds with one stone" with the forensic examination of the Target Computer. (See Doc. No. 134 at 6, 26.) The motion to modify (Doc. No. 107) was also unnecessary given Plaintiffs' irrational refusal to cooperate with Watchdog's EZ Imager proposal. (See Doc. No. 112-1 at 3-4, 7, 8, 15, 18-19, 22, 24, 29, 35, 38.) In sum, Plaintiffs' request for fees and costs would not be reasonable; would not directly relate to or result from the alleged spoliation; and would not be intended to compensate for the time or effort expended to obtain evidence on the Target Computer.

Accordingly, Plaintiffs' request for attorneys' fees is inappropriate.

(g) *Order compelling production of mirror image of Target Computer*

Finally, Plaintiffs request that the Court order ITA to provide a copy of the mirror image of the Target Computer to Plaintiffs' counsel. (See Doc. No. 134 at 2, 26.) This request should be rejected for several reasons:

First, Ms. Cantrell, who owns the Target Computer, strongly opposes having an image of her hard drive delivered to Plaintiffs or any of their agents. See Ex. D at ¶ 15.

Second, privacy concerns persist despite Plaintiffs' representations to the contrary. Fragments of data containing coherent sentences still remain on the Target Computer. There would be no way for Plaintiffs to unilaterally determine whether such fragments are from privileged communications between Watchdog and her counsel, among other files that should be off-limits. In fact, one of three fragments recovered from the Target Computer is part of a communication between Watchdog and her counsel. See Ex. N at ¶ 9. If Plaintiffs intend to scour through these fragments, they should be required to use ITA and to permit Watchdog's counsel to screen these fragments for privilege concerns.

Third, Plaintiffs' stated "need" (Doc. No. 134 at 26) of the image copy for this case can still be met by continuing to use ITA.

Finally, Plaintiffs' stated "need" (id.) of the image copy for the Montgomery County case is a concern that should be taken up by that court.

Accordingly, Plaintiffs' request that an image of the Target Computer's hard drive be delivered to their counsel is inappropriate.

IV. CONCLUSION

For the foregoing reasons, Watchdog respectfully requests that the Court deny Plaintiffs' Motion for Sanctions and enter an order in the attached, proposed form.

Respectfully,

By: s/

Jonathan Z. Cohen, Esquire (PA ID No. 205941)
303 West Lancaster Avenue # 144
Wayne, Pennsylvania 19087-3938
Tel.: (215) 901-7521
Fax: (215) 839-8951
Email: jzc@jzc-law.com

Attorney for Defendant Watchdog

Date: November 8, 2013

CERTIFICATE OF SERVICE

I, Jonathan Z. Cohen, attorney for Defendant Watchdog, certify that this document has been filed electronically and is available for viewing and downloading from the ECF system.

The following parties have consented to electronic service:

STANLEY B. CHEIKEN
Sbc@cheikenlawfirm.com

JONATHAN Z. COHEN
jzc@jzc-law.com

CHRISTA FRANK HIGH
chigh@mmwr.com, klemma@mmwr.com

NEIL E. JOKELSON
neil@jokelson.com, monica@jokelson.com, efile@jokelson.com, angela@jokelson.com

SIDNEY S. LIEBESMAN
sliebesman@mmwr.com

STEVEN PACHMAN
spachman@mmwr.com, cbutler@mmwr.com

K. CARRIE SARHANGI
csarhangi@mmwr.com, jmwright@mmwr.com

s/
Jonathan Z. Cohen, Esquire (PA ID No. 205941)

Attorney for Defendant Watchdog

Date: November 8, 2013